Intersite Authentication
or
What Does it Mean to Trust Another Site?

John Volmer
Argonne National Laboratory

Energy Sciences Coordinating Committee
Distributed Systems Management Working Group
ANL Document Release #93173

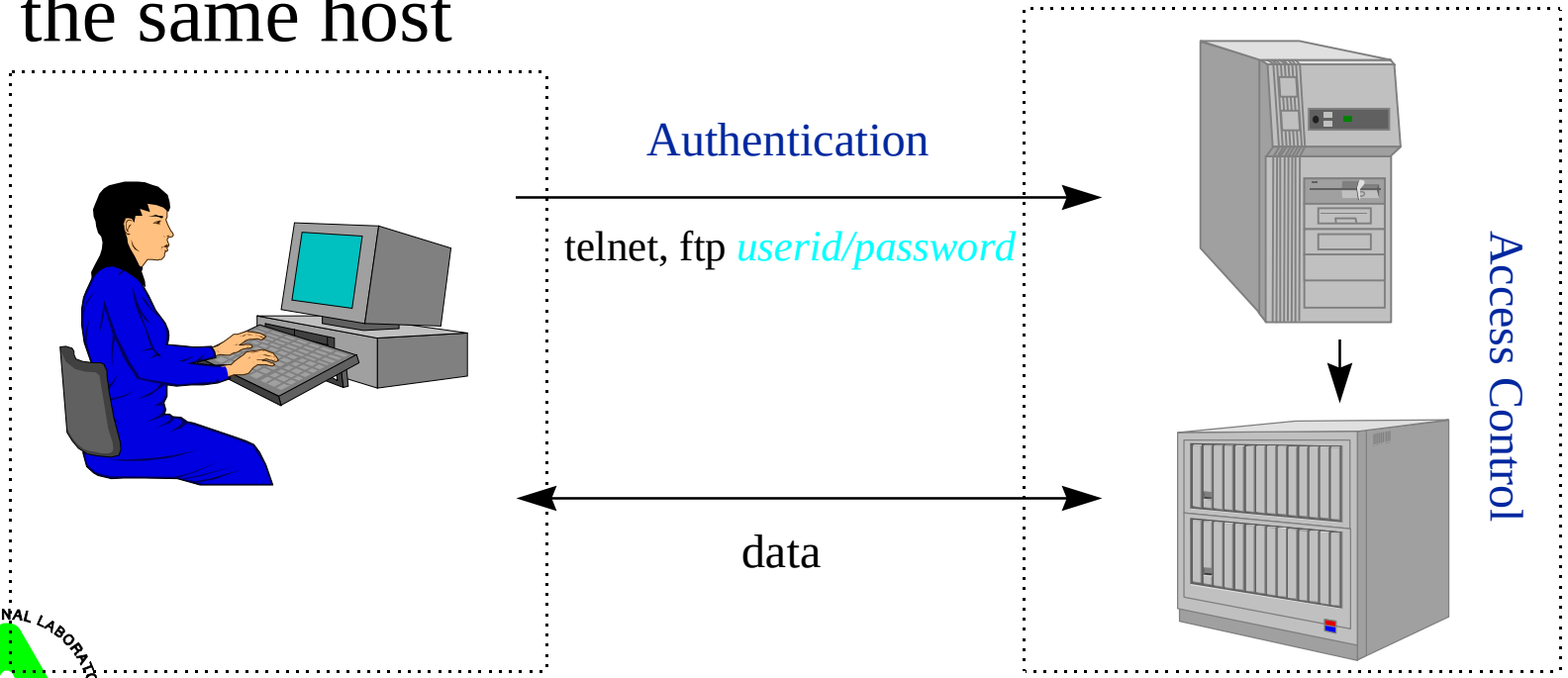
volmer@anl.gov
630.252.5449

Contents

- What's Changing?
- Implications of the change
  - Concerns
  - Opportunities
- Relevance of Intersite Trust
- So, What does it mean...
- The ESnet Approach
  - Plan
  - Highlights
  - Next Steps
- Conclusion

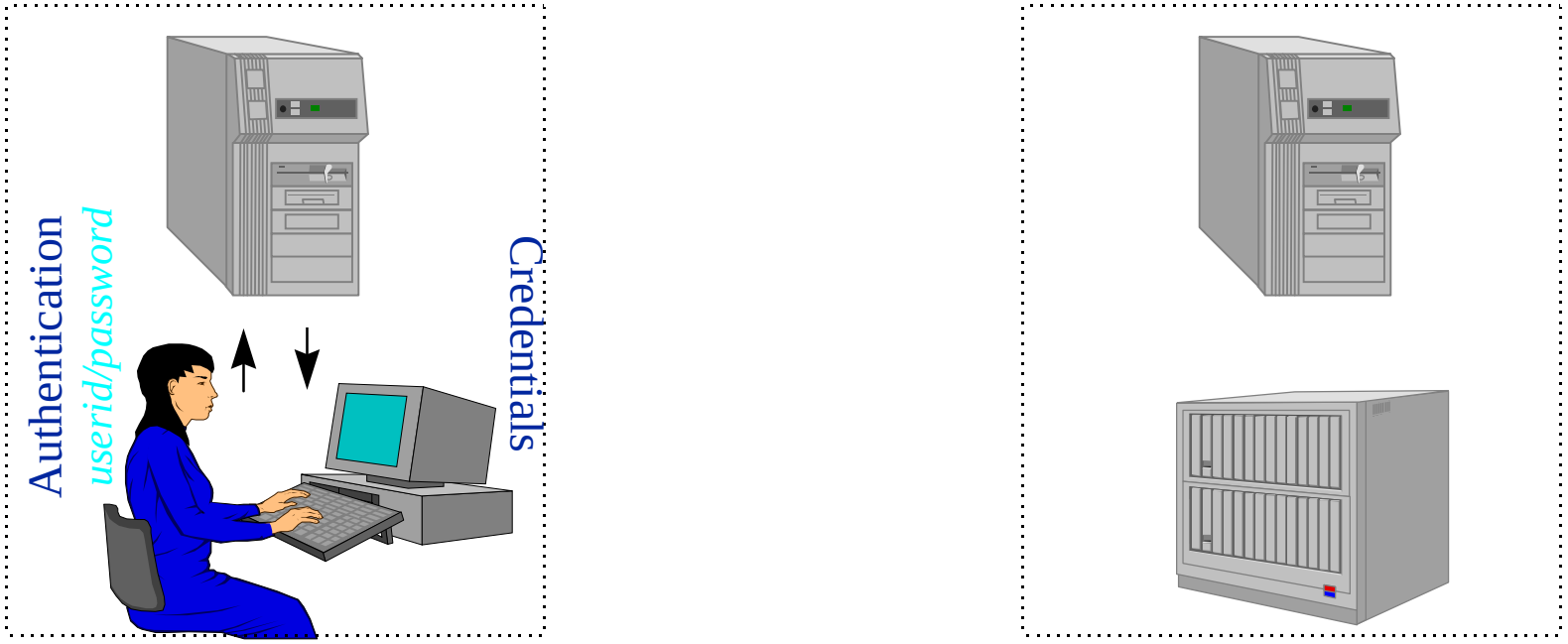
What's Changing?

- Presently authentication and resource access control were performed through the same organization; often the same host



What's Changing?

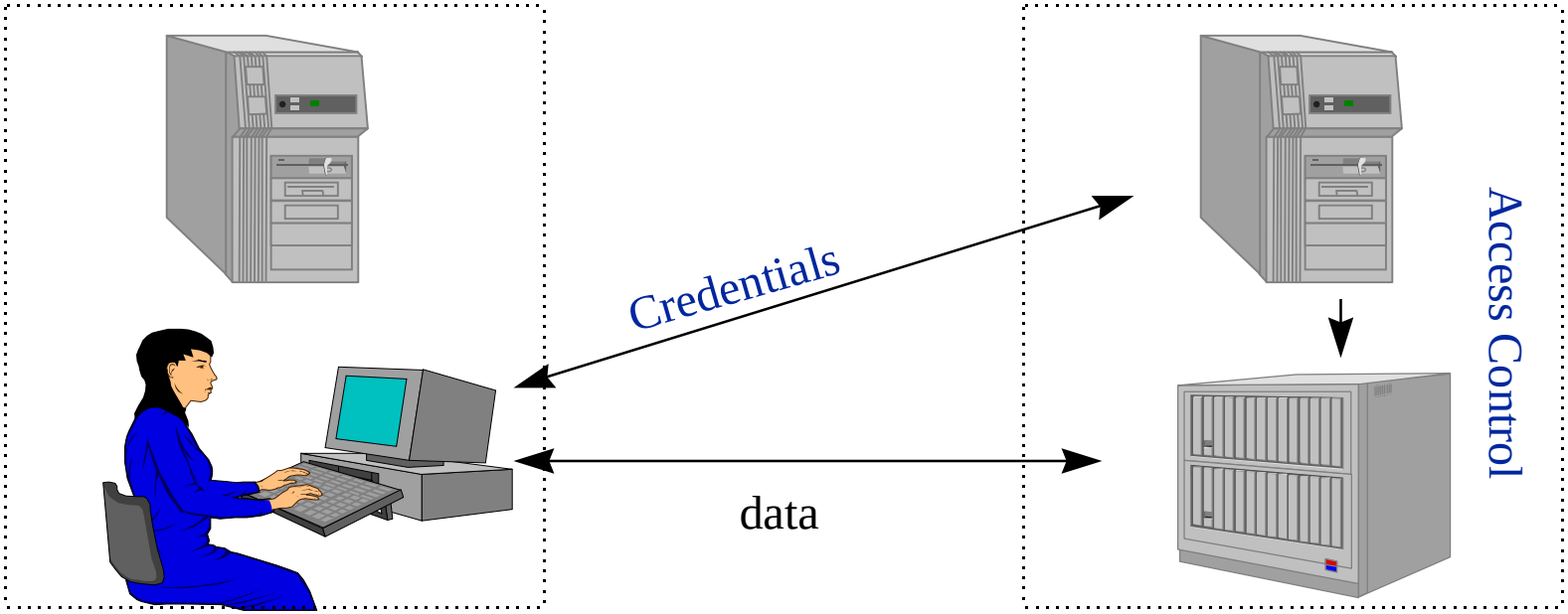
- Distributed authentication technologies permit users to authenticate locally and then …



Authentication is decoupled from access control

What's Changing (contd.)?

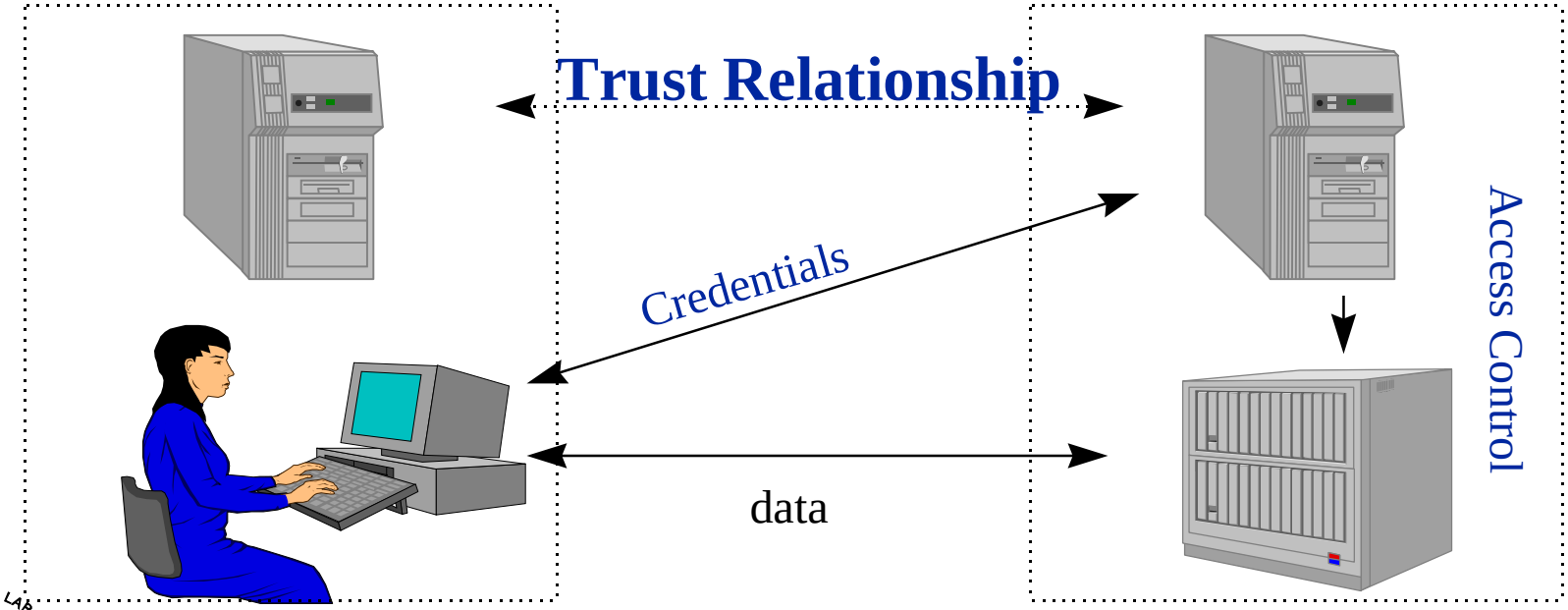
- … access resources at your site



Your access control mechanisms will trust credentials from other sites

What's Changing (contd.)?

- Your access control mechanisms will trust authentication mechanisms at other sites

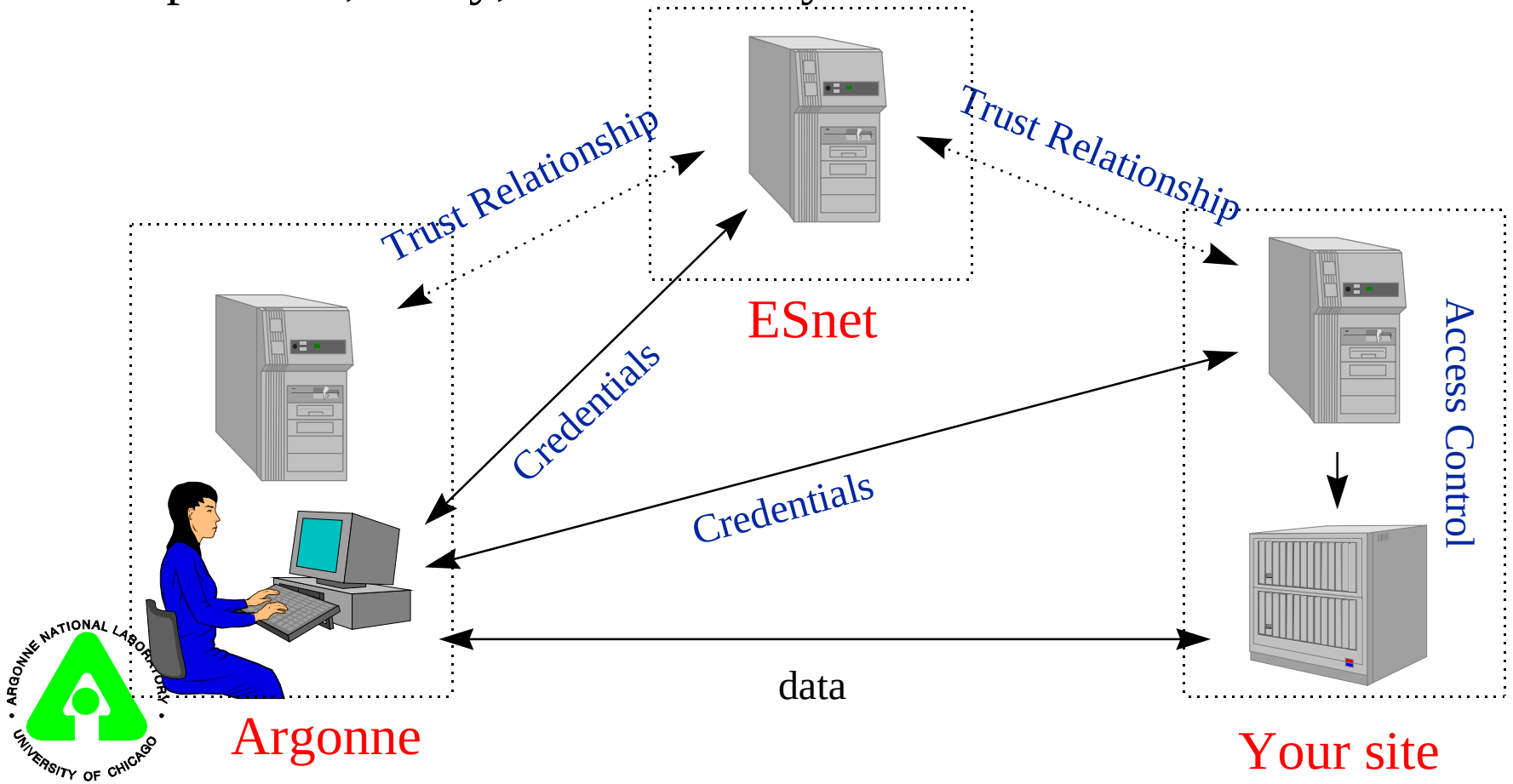


What's Changing (contd.)?

- Resources at your site will be protected with ACL's of the form
  - myfile rwl /…/dce.anl.gov/volmer

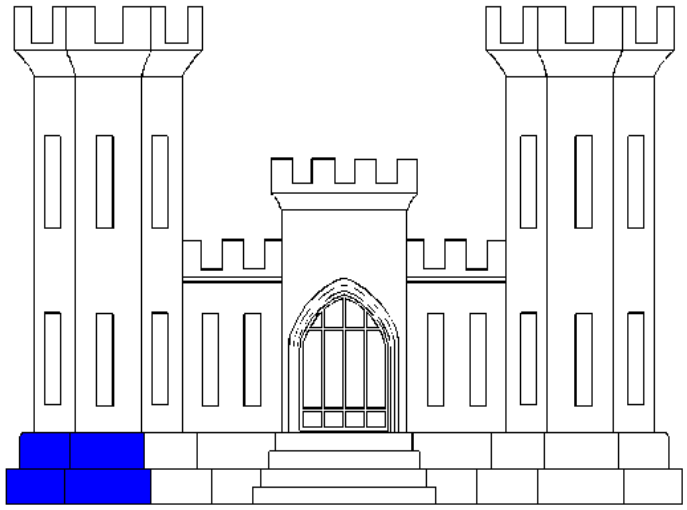
What's Changing (contd.)?

- Further, multi-party or transitive trust relationships are possible, likely, and necessary



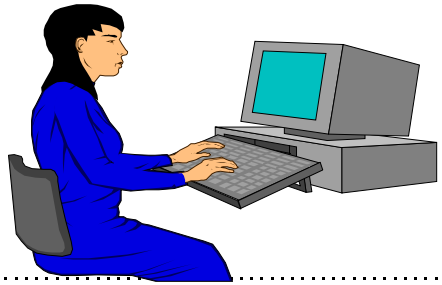
Implications

- My site will be a component of your computer protection plan
- In a transitive relationship, people you don't even know will be part of your protection plan
- How well I do my job affects how well you can do your job
  - Identified in the Final Report and Recommendation of the Esnet Authentication Pilot Project http://www.es.net/hypertext/authtf/documents.html



Implications (contd.)

- Concerns
  - People, policy, procedures, equipment outside your control are part of your computer protection policy



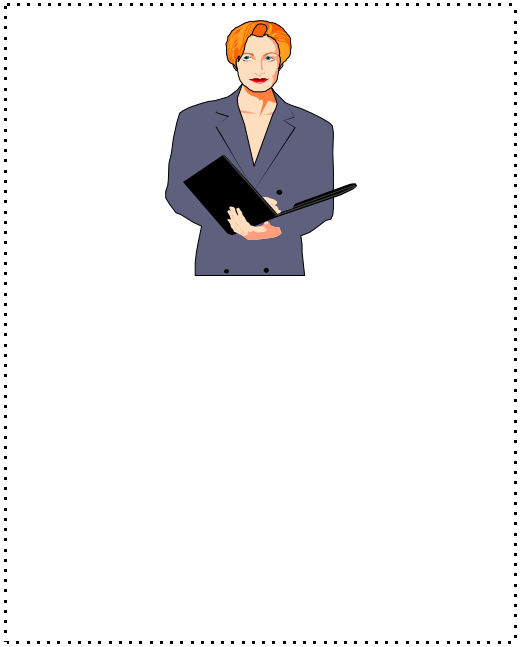
Argonne

Your site

Implications (contd.)

- Opportunities
  - There will now be a computer protection officer local to the user

Argonne



Your site

Relevance of Intersite Trust

- The issue of trust is a critical concept that must be addressed to enable wide area computing
- Trusting another site to authenticate a user is fundamental to
  - Distributed Computing Environment (DCE)
  - Public Key Infrastructure (PKI)

Relevance (contd.)

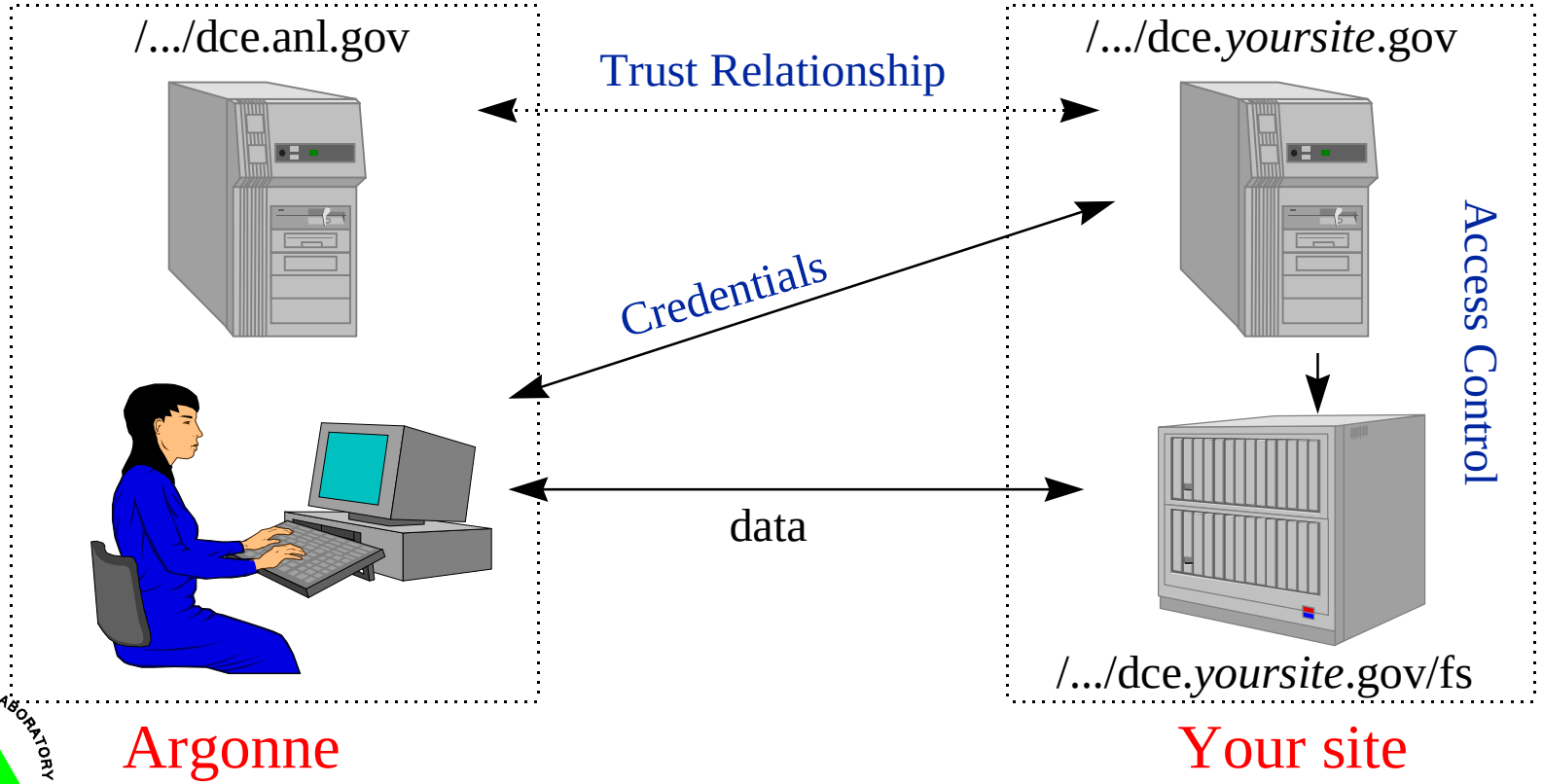
- Certifying that *these credentials* represent *this user* is essential for
  - Digital signature
  - Electronic commerce
  - Privacy
  - Wide area resource access control

Relevance of Intersite Trust

- Several DOE Laboratories need to support intersite collaborations with shared file systems (DCE and DFS)
  - ASCI Project
- Several DOE Laboratories plan to use PKI to enable secure communications
  - AMNII Project

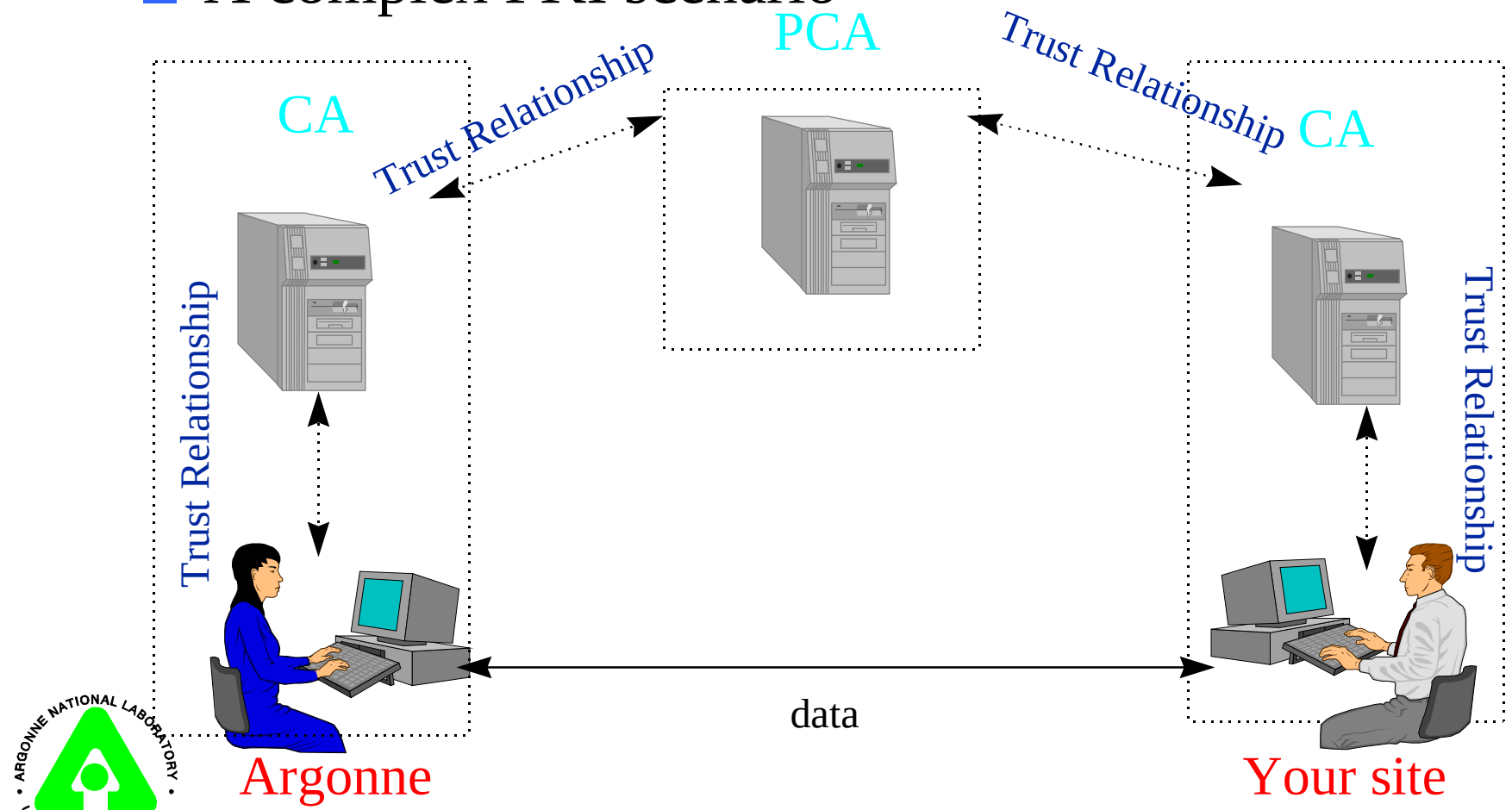
A DCE Scenario

- A simple DCE relationship



A PKI Scenario

- A complex PKI scenario



So, What does it Mean to *Trust* Another Site?

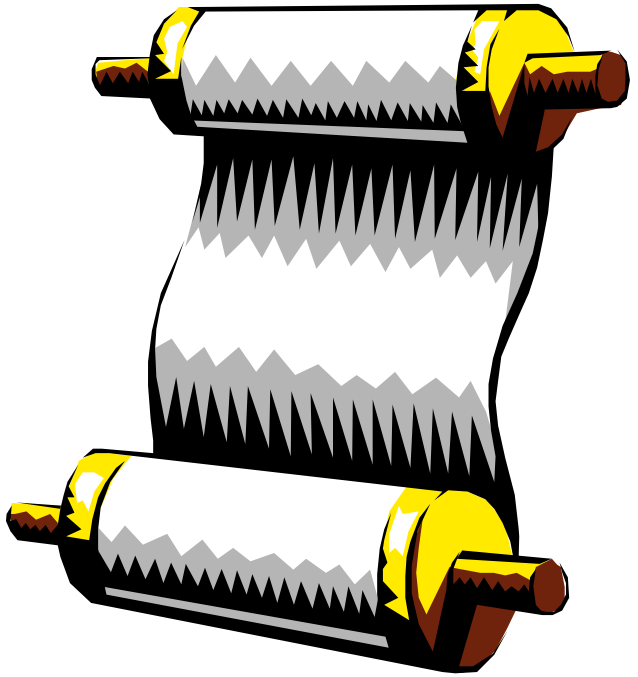
- Specifically
  - To be confident that the user was *correctly authenticated*
- Generally
  - To be able to predict another sites computer protection behavior

So, What Does it Mean to be *Correctly Authenticated*?

- To me, it means
  - The user is enrolled through my user enrollment process …
  - The user keeps his password secure …
  - My staff stays current on patches …
  - I safeguard the password repository …
  - etc.

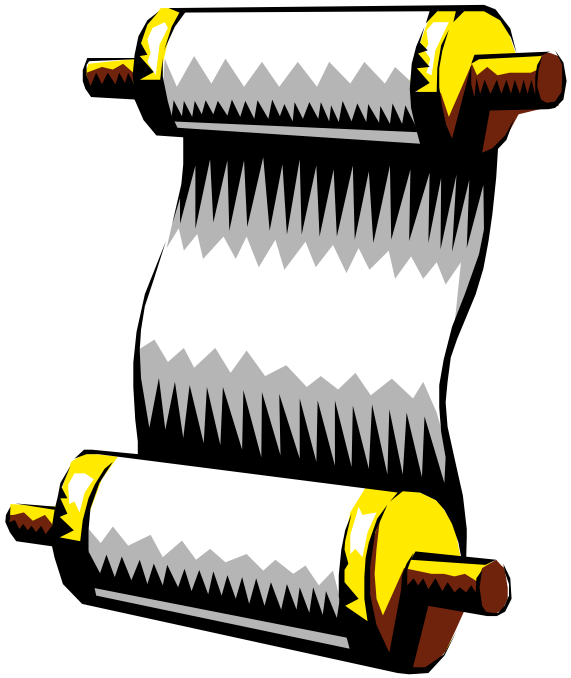
But …

- does it mean the same to you?
  - Is your user enrollment process as good as mine?
  - Do your user's safeguard their passwords as well as mine do?
  - Is your patch level as current as mine?
  - Do you safeguard your password repository as well as I do?
  - etc.



What a Minute …

- *Do you safeguard your password repository as well as I do???*
- There are a lot of policies and procedures involved in doing that!
- How do you compare policies and procedures?



How Do You Compare Policies and Procedures?

- This is the fundamental problem of intersite trust
  - How do you decide if two policies say the same thing?
  - How do you decide if two procedures have the same result?
  - How do you decide if a policy is complete?
- How do you do this for a dozen or more independent sites?
- You can't

But...

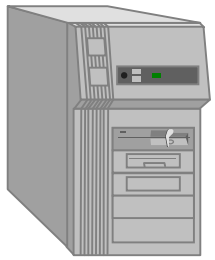
- We had something going for us:
  - We were all under the Department of Energy
  - DOE had developed base computer security requirements for all Laboratories
  - We had a minimum set of rules everyone already complied with!

So, Our Plan Was

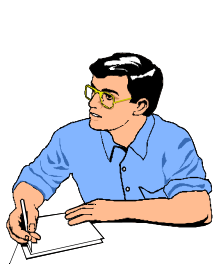
- Modify the base requirements with
  - Additions
  - Specifics
  - Deletions
- Make it so specific that any site was confident what the other site was doing
- Make it loose enough so that sites could comply

Plan (contd.)

- Target Sensitive Unclassified Data
  - A level of data of value
- In effect, what you would expect out of another site so that you could trust it to perform user authentication?



Argonne

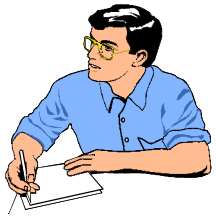


Your site

Risk Assessment Perspective

- Put yourself in the shoes of a sensitive data owner
- What you would expect out of another site so that you could trust it to perform user authentication?

?



Argonne

Your site

Make the requirements specific enough that data owners would feel safe

The Common Policy

- DOE 1360.2 and its associated orders
- A priori, each of the sites
  - already complied with these orders
  - they were a neutral starting point, and
  - considered them fairly complete
- Summarized in Draft 1989 Risk Assessment Guidelines

Modifications

- Held several meetings in 1996
- Used consensus review
- Progress
  - Version 0 policy issued in December 1995
  - Had Version 1 by May 8, 1996
  - Issued to DCE Working Group May 8, 1996
  - Developed Version 1.2 October 1996
  - 52 requirements
- Posted at http://www.es.net/hidden/dsmwg.html

Rules Cover an Assortment of Operational Requirements

- Protection of the KDC
- Password length and expiration
- Patch application
- Training of staff
- Compromise notification
- User enrollment

Highlights

- Weapons Laboratories vs. Energy Laboratories
  - Had higher requirements for user enrollment
    - » Required a badge
    - » Appear in person
  - Caused creation of a special DCE group
  - Special requirements for users to join this group

Highlights (contd.)

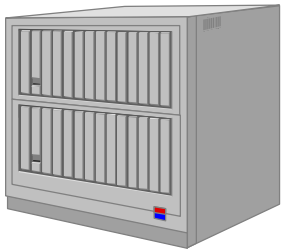
- Auditing
  - Necessary to maintain *trust*
  - Audit is limited to the standard
  - Audit is performed by other members of the community

Second Order Effects

- The standard identified several additional documents and tasks
  - What is the liability of authenticators or auditors?
  - Do we need a common user responsibilities statement?
  - How do new sites join the club?
  - What are staff training requirements?
  - etc.
- Some of these are now being addressed

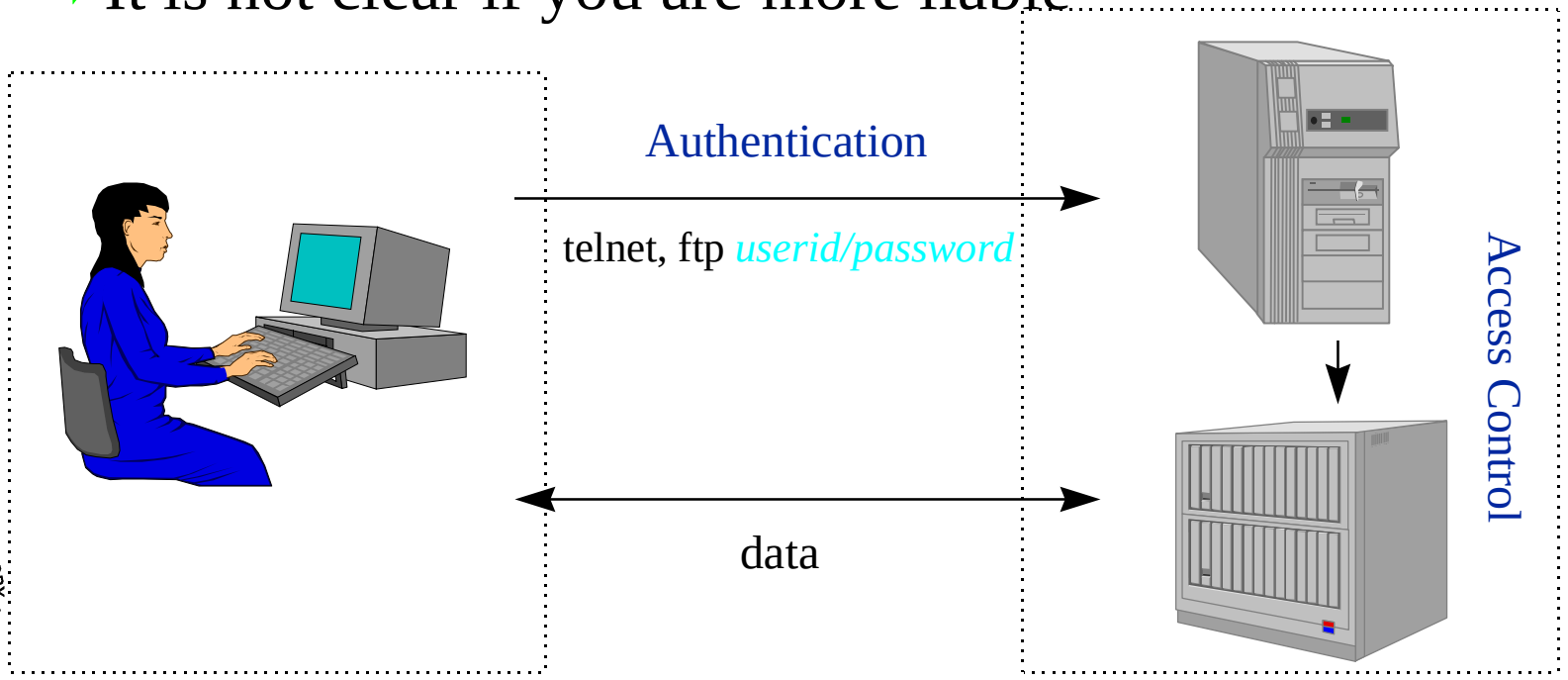
Liability of Authenticators and Auditors

- If a user presents credentials to my site that he is not authorized to have (violated my trust in your site) and uses them to take data or perform some action
  - Is your site liable for damages?
  - Are the auditors liable for damages?



Liability of Authenticators and Auditors

- Yes, and unknown
  - If you use a computer at another site, you are already liable today
  - It is not clear if you are more liable



User Responsibilities Statements

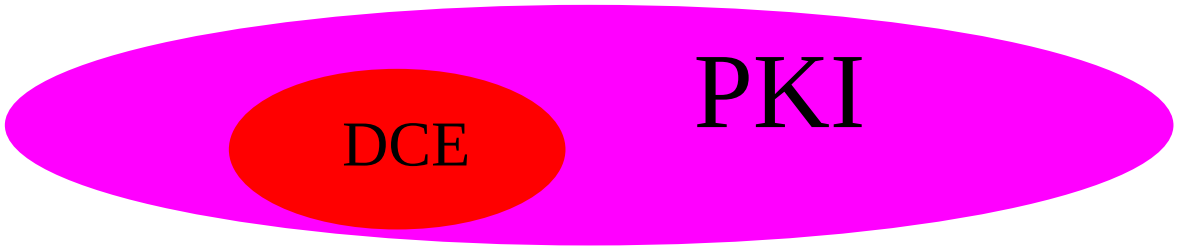
- We have an developed a comparison matrix
  - http://www.es.net/hidden/dsmwg.html

	Ames	ANL	Jefferson	etc.
Computer Use				
Monitoring				
Classified Work				
etc.				

- Just starting our analysis

Comparison with PKI Work

- This project is focused on DCE
- However, this work is a subset of the PKI issues
- Several papers exist by IETF and NIST on Certification Authority (CA) operation
  - http://csrc.nist.gov/pki
  - http://www.ietf.org/html.charters/pkix-charter.html
- We need to do a comparison



Co-conspirators

- Ames - A. Mikler
- LANL- R. Wilkins
- LLNL - B. Howard
- MITLNS - D. Woodruff
- PNNL - T. Harper, T. Thompson
- SNL - B. Jennings, P. Moore

The End

- Questions
- Comments
- Suggestions

http://www.es.net/hypertext/committees/dsmw.html